UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/511,105	10/14/2004	Jukka Tuomi	60091.00338	6584

32294 7590 06/13/2007

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
AJIBADE AKONAI, OLUMIDE	
ART UNIT	**PAPER NUMBER**
2617	

MAIL DATE	DELIVERY MODE
06/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/511,105	TUOMI ET AL.	
	Examiner	Art Unit	
	Olumide T. Ajibade-Akonai	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-14,21-23,25-38 and 45-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *2-12,14,21,25-36,38 and 45* is/are allowed.

6)☒ Claim(s) *13,22,23,37,46 and 47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 13, 22, 23, 37, 46, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McCann et al EP 1191763** (**hereinafter McCann**) in view of **Matsumoto et al 6,144,431** (**hereinafter Matsumoto**).

Regarding **claim 13**, McCann discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device (portable device, see fig. 1, col. 3, [0013]) to a service access point (communication between the portable device and the SSG using a secure communication protocol, see col. 3, [0015]); inputting identification data (WLAN identity, see fig. 1, col. 3, [0014]) of a subscriber of a mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]) to the service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]); checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]); and, if a valid access right exists, generating a password (PIN, see fig. 1, col. 3, [0017]), transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data (see fig. 1, col. 3, [0017]), and logging in to the service access point

from the data transfer device using the password transmitted to the subscriber terminal (mobile user utilizes the sent PIN for validation of WLAN account, see fig. 1, col. 3, [0017]).

McCann fails to disclose transmitting a second password from the service access point to the data transfer device over a data transfer connection, he second password being also used in connection with login.

In a similar field of endeavor, Matsumoto teaches a method of transmitting a second password (K1, see fig. 14, col. 18, lines 38-39) from the service access point (exchange 103-a) to the data transfer device (PS1, see fig. 14, col. 18, lines 33-36) over a data transfer connection, the second password being also used in connection with login (see col. 18, lines 33-47).

It would therefore have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teaching Matsumoto, by transmitting a second authentication key to mobile device for benefit of properly authorizing a mobile device in a specific service area.

Regarding **claim 22**, as applied to claim 1, McCann discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device (portable device, see fig. 1, col. 3, [0013]) to a service access point (communication between the portable device and the SSG using a secure communication protocol, see col. 3, [0015]); inputting identification data (WLAN identity, see fig. 1, col. 3, [0014]) of a subscriber of a mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]) to the service access point

(service selection gateway SSG 5, see fig. 1, col. 3, [0015]); checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]); and, if a valid access right exists, generating a password (PIN, see fig. 1, col. 3, [0017]), transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data (see fig. 1, col. 3, [0017]), and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal (mobile user utilizes the sent PIN for validation of WLAN account, see fig. 1, col. 3, [0017]).

McCann fails to disclose transmitting a user identification to the subscriber terminal corresponding to the mobile subscriber identification data and using the transmitted user identification in connection with login.

In the same field of endeavor, Matsumoto teaches transmitting a user identification (K1, see fig. 14, col. 18, lines 38-39) to the subscriber terminal (PS1, see fig. 14, col. 18, lines 33-36) corresponding to the mobile subscriber identification data (see fig. 2, 3 and 5, col. 18, lines 38-40) and using the transmitted user identification in connection with login (see col. 18, lines 33-47).

It would therefore have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teaching Matsumoto, by transmitting a second authentication key to mobile device for benefit of properly authorizing a mobile device in a specific service area.

Regarding **claim 23**, McCann discloses a method for authenticating a user

of a data transfer device, comprising: setting up a data transfer connection from the data transfer device (portable device, see fig. 1, col. 3, [0013]) to a service access point (communication between the portable device and the SSG using a secure communication protocol, see col. 3, [0015]); inputting identification data (WLAN identity, see fig. 1, col. 3, [0014]) of a subscriber of a mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]) to the service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]); checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]); and, if a valid access right exists, generating a password (PIN, see fig. 1, col. 3, [0017]), transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data (see fig. 1, col. 3, [0017]), and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal (mobile user utilizes the sent PIN for validation of WLAN account, see fig. 1, col. 3, [0017]).

McCann fails to disclose transmitting a user identification to the data transfer device corresponding to the mobile subscriber identification data and using the transmitted user identification in connection with login.

In the same field of endeavor, Matsumoto teaches transmitting a user identification (K1, see fig. 14, col. 18, lines 38-39) to the data transfer device (PS1, see fig. 14, col. 18, lines 33-36) corresponding to the mobile subscriber identification data

(see fig. 2, 3 and 5, col. 18, lines 38-40) and using the transmitted user identification in connection with login (see col. 18, lines 33-47).

It would therefore have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teaching Matsumoto, by transmitting a second authentication key to mobile device for benefit of properly authorizing a mobile device in a specific service area.

Regarding **claim 37**, McCann discloses a system for authenticating a user of a data transfer device, comprising: a data transfer device (handset 10, see col. 3, [0017]) a service access point that can be linked to the data transfer device over a first data transfer connection (service selection gateway SSG 5, see fig. 1, col. 3, [0015]), and an authentication server linked to the service access point over a second data transfer connection (visitor AAA unit 6, see fig. 1, col. 3, [0016]); transmitting the mobile subscriber identification data (WLAN identity, see fig. 1, col. 3, [0014]) to the authentication server over the second data transfer connection (see fig. 1, col. 3, [0016]); the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]) and, if a valid access right exists, to generate a password (PIN, see fig. 1, col. 3, [0017]) and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]).

McCann fails to disclose, wherein the authentication server is configured

to transmit a second from the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to use the user identification transmitted to the subscriber terminal in connection with login.

In the same field of endeavor, Matsumoto teaches wherein an authentication server (exchange 103-a) is configured to transmit a user identification (K1, see fig. 14, col. 18, lines 38-39) from the service access point (CS 109, see fig. 1, col. 7, lines 43-49) to the data transfer device (PS1, see fig. 14, col. 18, lines 33-36) over a data transfer connection and the data transfer device is configured to use the user identification transmitted to the subscriber terminal in connection with login (see col. 18, lines 33-47).

It would therefore have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teaching Matsumoto, by transmitting a second authentication key to mobile device for benefit of properly authorizing a mobile device in a specific service area.

Regarding **claim 46**, McCann discloses a system for authenticating a user of a data transfer device, comprising: a data transfer device (handset 10, see col. 3, [0017]) a service access point that can be linked to the data transfer device over a first data transfer connection (service selection gateway SSG 5, see fig. 1, col. 3, [0015]), and an authentication server linked to the service access point over a second data transfer connection (visitor AAA unit 6, see fig. 1, col. 3, [0016]); transmitting the mobile subscriber identification data (WLAN identity, see fig. 1, col. 3, [0014]) to the authentication server over the second data transfer connection (see fig. 1, col. 3,

[0016]); the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]) and, if a valid access right exists, to generate a password (PIN, see fig. 1, col. 3, [0017]) and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]).

McCann fails to disclose, wherein the authentication server is configured to transmit a user ID to the subscriber of the mobile communications system and the data transfer device is configured to use the user ID transmitted to the subscriber terminal in connection with login to the service access point.

In the same field of endeavor, Matsumoto teaches wherein a authentication server (exchange 103-a) is configured to transmit a user identification (K1, see fig. 14, col. 18, lines 38-39) to the subscriber of the mobile communications system (PS1, see fig. 14, col. 18, lines 33-36) and the data transfer device is configured to use the user identification transmitted to the subscriber terminal in connection with login to the service access point (see col. 18, lines 33-47).

It would therefore have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teaching Matsumoto, by transmitting a second authentication key to mobile device for benefit of properly authorizing a mobile device in a specific service area.

Regarding **claim 47**, McCann discloses a system for authenticating a user of a data transfer device, comprising: a data transfer device (handset 10, see col. 3, [0017]) a service access point that can be linked to the data transfer device over a first data transfer connection (service selection gateway SSG 5, see fig. 1, col. 3, [0015]), and an authentication server linked to the service access point over a second data transfer connection (visitor AAA unit 6, see fig. 1, col. 3, [0016]); transmitting the mobile subscriber identification data (WLAN identity, see fig. 1, col. 3, [0014]) to the authentication server over the second data transfer connection (see fig. 1, col. 3, [0016]); the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]) and, if a valid access right exists, to generate a password (PIN, see fig. 1, col. 3, [0017]) and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]).

McCann fails to disclose, wherein the authentication server is configured to transmit a user identification via the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to use the user identification transmitted to the subscriber terminal in connection with login to the service access point.

In the same field of endeavor, Matsumoto teaches wherein an

authentication server (exchange 103-a) is configured to transmit a user identification (K1, see fig. 14, col. 18, lines 38-39) via the service access point (CS 109, see fig. 1, col. 7, lines 43-49) to the data transfer device (PS1, see fig. 14, col. 18, lines 33-36) over a data transfer connection and the data transfer device is configured to use the user identification transmitted to the subscriber terminal in connection with login to the service access point (see col. 18, lines 33-47).

It would therefore have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the teaching Matsumoto, by transmitting a second authentication key to mobile device for benefit of properly authorizing a mobile device in a specific service area.

Allowable Subject Matter

3. Claims 2-12, 14, 21, 25-36, 38 and 45 are allowed.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gorsuch 6,526,034 discloses dual mode subscriber unit for short range, high rate and long range, lower rate data communications.

Song et al 7,065,067 discloses an authentication method between mobile node and home agent in a wireless communication system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Olumide T. Ajibade-Akonai whose telephone number is 571-272-6496. The examiner can normally be reached on M-F, 8.30p-5p.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rafael Perez-Gutierrez can be reached on 571-272-7915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OA
OA

Jemica M. Beamer

TEMICA BEAMER
PRIMARY EXAMINER